CLAIMS

1. A method of protecting content comprising:

receiving content at a device;

encrypting the content with a content key;

encrypting the content key with a domain key; and

storing the encrypted content key and the encrypted content.

2. A method of protecting content comprising:

receiving content at a device;

encrypting the content with a content key;

encrypting the content key with a domain key; and

storing a voucher associated with the content;

wherein the voucher includes the encrypted content key and a usage state record.

3. The method according to claim 2 wherein the voucher also contains a domain traversal flag.

4. The method according to claim 2 wherein the content is encrypted before the content is received at the device.

5. A method of protecting content comprising:

receiving content at a device;

receiving a usage state record associated with the content;

receiving a domain traversal flag associated with the content;

encrypting the content with a content key;

encrypting the content key with a device key if the usage state record indicates that usage is not unrestricted;

encrypting the content key with a domain key if the domain traversal flag indicates that domain traversal is forbidden; and

storing a voucher associated with the content:

wherein the voucher contains the encrypted content key, the usage state record, and the domain traversal flag.

6. The method according to claim 5 further comprising:

protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

7. A method of moving protected content within an authorized domain comprising:

transmitting encrypted content and a voucher associated with said encrypted content from a first device in the authorized domain to a second device in the authorized domain;

the voucher including an encrypted content key and a usage state record;

at the first device rendering any vouchers associated with said encrypted content unusable.

8. The method of claim 7 further comprising:

encrypting the entire voucher.

9. The method of claim 7 further comprising:

receiving said encrypted content and the voucher associated with that content in a second device in the authorized domain.

10. The method of claim 9 comprising:

decrypting the encrypted content key at the second device; and

using the decrypted content key to decrypt the encrypted content.

11. A method for moving protected content from a first device in one authorized domain to a target device in a different authorized domain comprising:

checking a voucher associated with a piece of content;

the voucher including an encrypted content key, a usage state record and a domain traversal flag;

if the usage state record allows moving,

decrypting the encrypted content key with a device key; and

encrypting the decrypted content key with the public key of the target device;

replacing the original encrypted content key with the re-encrypted content key in the voucher;

transmitting encrypted content and the amended voucher to the target device; and

at the first device rendering any vouchers associated with the content unusable.

12. The method of claim 11 where the device key used to decrypt the encrypted content key is a private key of the first device.

13. The method of claim 11 further comprising:

decrypting the voucher received at the target device using a private key associated with the target device's public key;

decrypting the encrypted content using the decrypted content key from the voucher.

14. A method of copying protected content within an authorized domain to a target device within said authorized domain comprising:

at a first device within the authorized domain, checking a usage state record contained in a voucher associated with a piece of encrypted content;

the voucher including a usage state record, and an encrypted content key;

if the usage state record is not unrestricted and allows copying:

decrypting the encrypted content key with a device key;

re-encrypting the decrypted content key with a public key of the target device;

updating the usage state record ; and

storing the re-encrypted content key and the updated usage state record in a re-targeted voucher; and

sending the encrypted content and the re-targeted voucher to the target device.

15. The method of claim 14 where the device key used to decrypt the encrypted content key is a private key of the first device.

16. The method of claim 14 further comprising:

receiving the encrypted content and re-targeted voucher at the target device;

decrypting the re-encrypted content key using a domain key;

decrypting the encrypted content with the content key.

17. The method of claim 16 further comprising:

decrypting the re-encrypted content key with a private key of the target device.

18. The method of claim 14 wherein the usage state record contains a budget of allowed copies and further comprising reducing the budget of allowed copies.

19. A method for copying protected content from a device in a first authorized domain to a target device in a second authorized domain comprising:

in a first device within the first authorized domain, checking a usage state record contained in a voucher associated with a piece of encrypted content, wherein the voucher also includes an encrypted content key;

if the usage state record or a domain traversal flag in said voucher indicates that inter-domain copying is allowed,

decrypting the encrypted content key with a device key;

re-encrypting the decrypted content key with a public key from the target device;

updating the usage state;

storing the updated usage state and the re-encrypted content key in a re-targeted voucher; and

transmitting encrypted content and the re-targeted voucher to the target device.

20. The method of claim 19 where the device key used to decrypt the encrypted content key is a private key of the first device.

21. The method of claim 19 further comprising:

protecting at least part of the re-targeted voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

22. The method of claim 19 wherein the usage state record contains a budget of allowed copies and further comprising:

reducing the budget of allowed copies.

23. A method of identifying protected content while maintaining backwards compatibility comprising:

receiving content;

checking if content is watermarked;

encrypting the content with a content key if the content is watermarked.

24. The method of claim 23 further comprising:

receiving usage information and an associated content ID;

checking the watermark to see if a content ID contained therein matches the content ID associated with the usage information;

treating the content as completely restricted if content ID associated with the usage information does not match the content ID contained in the watermark.

25. The method of claim 24 wherein the usage information includes a usage state record and a domain traversal flag.

26. The method of claim 23 further comprising:

removing the watermark from the content.

27. The method of claim 24 further comprising:

removing the watermark from the content.

28. A method of using protected content comprising:

decrypting an encrypted content key with a domain key;

decrypting an associated piece of content with the decrypted content key; and

rendering the decrypted content.

29. The method of claim 28 further comprising:

decrypting the encrypted content key with a private key.

30. A method of protecting content comprising:

receiving content at a device;

receiving a content key seed at the device;

creating a content key by operating on the content key seed with a domain key;

encrypting the content with the content key;

encrypting the content key with the domain key; and

storing the encrypted content key and the encrypted content.

31. The method of claim 30 further comprising:

receiving a content ID and usage information;

creating a voucher including the encrypted content key, the content ID, a domain

ID, and usage information.

32. The method of claim 31 further comprising:

protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

33. The method of claim 30 where the act of operating on the content key seed with a domain key is accomplished by encrypting the content key seed with the domain key.

34. A method of creating a content key comprising:

operating on a content key seed with a domain key;

35. The method of claim 34 further comprising:

receiving a content ID and a domain ID;

using the content ID to determine the content key seed;

using the domain ID to determine the domain key.

36. The method of claim 34 further comprising:

using a content ID to generate the content key seed.

37. A method for registering an authorized device in an authorized domain comprising:

transmitting information about the unregistered authorized device and the

authorized domain to a trust management provider;

receiving certification from the trust management provider to add said authorized device to the authorized domain as a registered device.

38. The method of claim 37 further comprising:

the trust management provider contacting a third party to obtain the requirements of the authorized domain.

39. The method of claim 37 further comprising:

receiving information about the unregistered authorized device at a registered authorized device already a part of the authorized domain.

40. A method of certifying the transfer of content out of an authorized device comprising:

receiving a request to transfer content from a first authorized device to a second authorized device;

contacting a trust management provider to verify the protection employed at the second authorized device;

if trust management provides authorization, transferring content.

41. The method of claim 40 further comprising:

the trust management provider contacting a third party to discern the protection required for the transfer to be authorized.

42. A method of providing payment in a superdistribution system comprising:

transferring content from a first device to a second device;

the second device contacting a trust management provider to purchase usage rights for the content;

the trust management provider distributing proceeds from the purchase.

43. The method of claim 42 where more than one party receives proceeds from the purchase.

44. The method of claim 42 where a content provider receives some portion of the proceeds of the purchase.

45. The method of claim 42 where users of the first device receive some portion of the proceeds of the purchase.

46. The method of claim 42 further comprising:

the trust management provider contacting the owner of the content to determine the terms of the purchase.

47. A method of checking the integrity of a voucher comprising:

receiving the voucher at a first device from a second device;

computing a cryptographic hashing function over at least part of the voucher;

decrypting an encrypted hash value stored in the voucher with a public key of the

second device;

comparing the computed hash value with the stored hash value.

48. The method of claim 47 where if the computed hash value does not equal the stored hash value, indicating that the voucher has been tampered with.

49. The method of claim 47 where the act of indicating the voucher has been tampered with includes making the content unusable.

50. An article manufacture comprising:

a computer readable medium comprising instructions for:

receiving content at a device;

encrypting the content with a content key;

encrypting the content key with a domain key; and

storing the encrypted content key and the encrypted content.

51. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving content at a device;

encrypting the content with a content key;

encrypting the content key with a domain key; and

storing a voucher associated with the content;

wherein the voucher includes the encrypted content key and a usage state record.

52. The article of manufacture of claim 51 wherein the voucher also contains a domain traversal flag.

53. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving content at a device;

receiving a usage state record associated with the content;

receiving a domain traversal flag associated with the content;

encrypting the content with a content key;

encrypting the content key with a device key if the usage state record indicates that usage is not unrestricted;

encrypting the content key with a domain key if the domain traversal flag indicates that domain traversal is forbidden; and

storing a voucher associated with the content:

wherein the voucher contains the encrypted content key, the usage state record, and the domain traversal flag.

54. The computer readable medium of claim 53 further comprising instructions for:

protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

55. An article of manufacture comprising:

a computer readable medium comprising instructions for:

transmitting encrypted content and a voucher associated with said encrypted content from a first device in an authorized domain to a second device in the authorized domain;

the voucher including an encrypted content key and a usage state record;

at the first device rendering any vouchers associated with said encrypted content unusable.

56. The computer readable medium of claim 55 further comprising instructions for:

encrypting the entire voucher.

57. An article of manufacture comprising:

a computer readable medium comprising instructions for:

on a first device checking a voucher associated with a piece of content;

the voucher including an encrypted content key, a usage state record and a domain traversal flag;

if the usage state record allows moving,

decrypting the encrypted content key with a device key; and

encrypting the decrypted content key with the public key of a target device;

replacing the original encrypted content key with the re-encrypted content key in the voucher;

transmitting encrypted content and the amended voucher to the target device; and

rendering any remaining vouchers associated with the content unusable.

58. The article of manufacture of claim 57 where the device key used to decrypt the encrypted content key is a private key of the first device.

59. An article of manufacture comprising:

a computer readable medium comprising instructions for:

checking a usage state record contained in a voucher associated with a piece of encrypted content;

the voucher including a usage state record, and an encrypted content key;

if the usage state record is not unrestricted and allows copying:

decrypting the encrypted content key with a device key;

re-encrypting the decrypted content key with a public key of a target device;

updating the usage state record ; and

storing the re-encrypted content key and the updated usage state record in a re-targeted voucher; and

sending the encrypted content and the re-targeted voucher to the target device.

60. The article of manufacture of claim 59 where the device key used to decrypt the encrypted content key is a private key of the first device.

61. The article of manufacture of claim 59 wherein the usage state record contains a budget of allowed copies and further comprising reducing the budget of allowed copies.

62. An article of manufacture comprising:

a computer readable medium comprising instructions for:

checking a usage state record contained in a voucher associated with a piece of encrypted content, wherein the voucher also includes an encrypted content key;

if the usage state record or a domain traversal flag in said voucher indicates that inter-domain copying is allowed,

decrypting the encrypted content key with a device key;

re-encrypting the decrypted content key with a public key from a target device;

updating the usage state;

storing the updated usage state and the re-encrypted content key in a re-targeted voucher; and

transmitting encrypted content and the re-targeted voucher to the target device.

63. The article of manufacture of claim 62 where the device key used to decrypt the encrypted content key is a private key of the first device.

64. The computer readable medium of claim 62 further comprising instructions for:

protecting at least part of the re-targeted voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

65. The article of manufacture of claim 62 wherein the usage state record contains a budget of allowed copies and the computer readable medium further comprising instructions for:

reducing the budget of allowed copies.

66. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving content;

checking if content is watermarked;

encrypting the content with a content key if the content is watermarked.

67. The computer readable medium of claim 66 further comprising instructions for:

receiving usage information and an associated content ID;

checking the watermark to see if a content ID contained therein matches the

content ID associated with the usage information;

treating the content as completely restricted if content ID associated with the usage information does not match the content ID contained in the watermark.

68. The article of manufacture of 67 wherein the usage information includes a usage state record and a domain traversal flag.

69. The computer readable medium of claim 66 further comprising instructions for:

removing the watermark from the content.

70. The computer readable medium of claim 67 further comprising instructions for:

removing the watermark from the content.

71. An article of manufacture comprising:

a computer readable medium comprising instructions for:

decrypting an encrypted content key with a domain key;

decrypting an associated piece of content with the decrypted content key; and

rendering the decrypted content.

72. The computer readable medium of claim 71 further comprising instructions for:

decrypting the encrypted content key with a private key.

73. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving content at a device;

receiving a content key seed at the device;

creating a content key by operating on the content key seed with a domain key;

encrypting the content with the content key;

encrypting the content key with the domain key; and

storing the encrypted content key and the encrypted content.

74. The computer readable medium of claim 73 further comprising instructions for:

receiving a content ID and usage information;

creating a voucher including the encrypted content key, the content ID, a domain ID, and usage information.

75. The computer readable medium of claim 74 further comprising instructions for:

protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

76. The article of manufacture of claim 73 where the act of operating on the content key seed with a domain key is accomplished by encrypting the content key seed with the domain key.

77. An article of manufacture comprising:

a computer readable medium comprising instructions for:

operating on a content key seed with a domain key;

78. The computer readable medium of claim 77 further comprising instructions for:

receiving a content ID and a domain ID;

using the content ID to determine the content key seed;

using the domain ID to determine the domain key.

79. The computer readable medium of claim 77 further comprising instructions for:

using a content ID to generate the content key seed.

80. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving information about an unregistered authorized device and an authorized domain;

transmitting certification from to add said authorized device to the authorized domain as a registered device.

81. The computer readable medium of claim 80 further comprising instructions for:

contacting a third party to obtain the requirements of the authorized domain.

82. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving a request to transfer content from a first authorized device to a second authorized device;

contacting a trust management provider to verify the protection employed at the second authorized device;

if trust management provides authorization, transferring content.

83. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving requests to purchase usage rights for a piece of content;

distributing proceeds from the purchase.

84. The article of manufacture of claim 83 where more than one party is sent proceeds from the purchase.

85. The article of manufacture of claim 83 where a content provider is sent some portion of the proceeds of the purchase..

86. The computer readable medium of claim 83 further comprising instructions for:

the trust management provider contacting the owner of the piece ofcontent to determine the terms of the purchase.

87. An article of manufacture comprising:

a computer readable medium comprising instructions for:

receiving a voucher from a second device;

computing a cryptographic hashing function over at least part of the voucher;

decrypting an encrypted hash value stored in the voucher with a public key of the second device;

comparing the computed hash value with the stored hash value.

88. The article of manufacture of claim 87 where if the computed hash value does not equal the stored hash value, indicating that the voucher has been tampered with.

89. The article of manufacture of claim 87 where the act of indicating the voucher has been tampered with includes making the content unusable.

90. An apparatus capable of protecting content comprising:

means for receiving content at said appartus;

means for encrypting the content with a content key;

means for encrypting the content key with a domain key; and

means for storing the encrypted content key and the encrypted content.

91. An apparatus capable of protecting content comprising:

means for receiving content at said appartus;

means for encrypting the content with a content key;

means for encrypting the content key with a domain key; and

means for storing a voucher associated with the content;

wherein the voucher includes the encrypted content key and a usage state record.

92. The apparatus of claim 91 wherein the voucher also contains a domain traversal flag.

93. An apparatus for protecting content comprising:

means for receiving content at said apparatus;

means for receiving a usage state record associated with the content;

means for receiving a domain traversal flag associated with the content;

means for encrypting the content with a content key;

means for encrypting the content key with a device key if the usage state record indicates that usage is not unrestricted;

means for encrypting the content key with a domain key if the domain traversal flag indicates that domain traversal is forbidden; and

means for storing a voucher associated with the content:

wherein the voucher contains the encrypted content key, the usage state record, and the domain traversal flag.

94. The apparatus of claim 93 further comprising:

means for protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

95. An apparatus capable of moving protected content within an authorized domain comprising:

means for transmitting encrypted content and a voucher associated with said encrypted content from said apparatus to a second device in the authorized domain;

the voucher including an encrypted content key and a usage state record;

means for rendering any vouchers associated with said encrypted content unusable.

96. The apparatus of claim 95 further comprising:

means for encrypting the entire voucher.

97. An apparatus capable of moving protected content to a target device in a different authorized domain comprising:

means for checking a voucher associated with a piece of content;

the voucher including an encrypted content key, a usage state record and a domain traversal flag;

means for decrypting the encrypted content key with a device key;

means for encrypting the decrypted content key with the public key of the target device;

means for replacing the original encrypted content key with the re-encrypted content key;

means for transmitting encrypted content and the amended voucher to the target device; and

means for rendering any vouchers associated with the content unusable.

98. The apparatus claim 97 where the device key used to decrypt the encrypted content key is a private key of the apparatus.

99. An apparatus for copying protected content within an authorized domain to a target device within said authorized domain comprising:

means for checking a usage state record contained in a voucher associated with a piece of encrypted content;

the voucher including a usage state record, and an encrypted content key;

means for decrypting the encrypted content key with a device key;

means for re-encrypting the decrypted content key with a public key of the target device;

means for updating the usage state record ;

means for storing the re-encrypted content key and the updated usage state record in re-targeted voucher; and

means for sending the encrypted content and the re-targeted voucher to the target device.

100. The apparatus of claim 99 where the device key used to decrypt the encrypted content key is a private key of the first device.

101. The apparatus of claim 99 wherein the usage state record contains a budget of allowed copies and further comprising reducing the budget of allowed copies.

102. An apparatus capable of copying protected content to a target device in a second authorized domain comprising:

means for checking a usage state record contained in a voucher associated with a piece of encrypted content, wherein the voucher also includes an encrypted content key;

means for decrypting the encrypted content key with a device key;

means for re-encrypting the decrypted content key with a public key from the target device;

means for updating the usage state;

means for storing the updated usage state and the re-encrypted content key in a re-targeted voucher; and

means for transmitting encrypted content and the re-targeted voucher to the target device.

103. The apparatus of claim 102 where the device key used to decrypt the encrypted content key is a private key of the first device.

104. The apparatus of claim 102 further comprising:

means for protecting at least part of the re-targeted voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

105. The apparatus of claim 102 wherein the usage state record contains a budget of allowed copies and further comprising:

means for reducing the budget of allowed copies.

106. An apparatus capable of identifying protected content while maintaining backwards compatibility comprising:

means for receiving content;

means for checking if content is watermarked;

means for encrypting the content with a content key if the content is watermarked.

107. The apparatus of claim 106 further comprising:

means for receiving usage information and an associated content ID;

means for checking the watermark to see if a content ID contained therein matches the content ID associated with the usage information;

means for treating the content as completely restricted if content ID associated with the usage information does not match the content ID contained in the watermark.

108. The apparatus of claim 107 wherein the usage information includes a usage state record and a domain traversal flag.

109. The apparatus of claim 106 further comprising:

means for removing the watermark from the content.

110. The apparatus of claim 107 further comprising:

means removing the watermark from the content.

111. An apparatus for using protected content comprising:

means for decrypting an encrypted content key with a domain key;

means for decrypting an associated piece of content with the decrypted content key; and

means for rendering the decrypted content.

112. The apparatus of claim 111 further comprising:

means for decrypting the encrypted content key with a private key.

113. An apparatus for protecting content comprising:

means for receiving content at said apparatus;

means for receiving a content key seed at the apparatus;

means for creating a content key by operating on the content key seed with a domain key;

means for encrypting the content with the content key;

means for encrypting the content key with the domain key; and

means for storing the encrypted content key and the encrypted content.

114. The apparatus of claim 113 further comprising:

means for receiving a content ID and usage information;

means for creating a voucher including the encrypted content key, the content ID, a domain ID, and usage information.

115. The apparatus of claim 114 further comprising:

means for protecting at least part of the voucher using at least one of the following:

a cryptographic hashing function; or

a digital signature.

116. The apparatus of claim 113 where the means for operating on the content key seed with a domain key is accomplished by encrypting the content key seed with the domain key.

117. An apparatus for creating a content key comprising:

means for operating on a content key seed with a domain key;

means for receiving a content ID and a domain ID;

means for using the content ID to determine the content key seed;

means using the domain ID to determine the domain key.

118. The apparatus of claim 117 further comprising:

means for using a content ID to generate the content key seed.

119. An apparatus capable of registering an authorized device in an authorized domain comprising:

means for receiving information about the unregistered authorized device and the authorized domain to a trust management provider;

means for transmitting certification from the trust management provider to add said authorized device to the authorized domain as a registered device.

120. An apparatus capable of checking the integrity of a voucher comprising:

means for receiving a voucher from a second device;

means for computing a cryptographic hashing function over at least part of the voucher;

means for decrypting an encrypted hash value stored in the voucher with a public key of the second device;

means for comparing the computed hash value with the stored hash value.

121. The apparatus of claim 120 further comprising:

means for indicating that the voucher has been tampered with.

122. The apparatus of claim 120 where the means for indicating the voucher has been tampered with includes making the content unusable.